



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,174	01/21/2004	Akashi Satoh	JP920020242US1	4993
7590 Ryan, Mason & Lewis, LLP 90 Forest Avenue Locust Valley, NY 11560		04/24/2007	EXAMINER MAI, TAN V	
			ART UNIT 2193	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		04/24/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/762,174 Examiner Tan V. Mai	SATOH ET AL. Art Unit 2193

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 15 February 2007.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-13 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-13 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 26 March 2004 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>2/21/04</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
|  | 6) <input type="checkbox"/> Other: _____                                    |

Art Unit: 2193

1. Applicant's election with traverse of Species I, Claims 1-4 and 9-12, in Paper dated 2/15/07 is acknowledged. Because applicant traverse on the ground that the species are not patentably distinct, i.e., the "Wallace tree bock" (species I) and "multiplication means" (species II) are at least part of Wallace tree block 110 in Fig. 7. Therefore, claims 1-13 are examined together.

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-4 and 9-12 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for "Wallace tree block ... adding the partial products into a carr save form", does not reasonably provide enablement for "Wallace tree block ... adding the partial products into a redundant binary form". The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the invention commensurate in scope with these claims.

The applicants have failed to disclose the physical structure of their multiplier / cipher circuit with any meaningful degree of specificity.

The examiner contends that not only would it require undue experimentation to design the above multiplier / cipher circuit which would perform the function(s) disclosed and claimed, but that it would also require undue experimentation for one of ordinary skill in the art to design working apparatus that would permit the "Wallace tree block ... adding the partial products into a redundant binary form". It is noted that "redundant binary" is representation of [-1, 0 +1].

Art Unit: 2193

3. Claims 1-4 and 9-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per independent claims 1 and 9, the phrases "redundant binary form" are misdescriptive because the specification does NOT support them. Also, claims 1 and 9 seem to be incomplete in that they recite only a portion of the methodology required for the multiplier / cipher circuit to become operational, i.e., they omit essential elements and/or steps. It is noted that the preamble of claims 1 and 9 recite "multiplier / cipher circuit". Therefore, the [final] results should be products. See MPEP 2172.01.

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

((b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1 and 3-4 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Kelley et al.

As per independent claim 1, Kelley et al teach, e.g., see Figs. 3-8, the claimed combination. The circuit comprises "...reduction tree" (element 524 of Fig. 3), sum register (530) and (carry register (535) and adder (560). Also, see col. 1, line 63 to col. 2, line 44 [for Wallace tree], and col. 6 line 45 to col. 7, line 9, especially lines 45-54, i.e., "accumulated sum" and "accumulated carry" for the claimed "sum calculation block" and "carry calculation block", respectively.

As per dependent claims 3-4, Kelley et al teach the detail features.

Art Unit: 2193

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2 and 5-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kelley et al.

Kelley et al have been discussed in paragraph 4 above.

As per dependent claim 2, the claim adds the "sum calculation block ... multiplication over an extension field of two". The Wallace tree technique, i.e., carry save adder, is well known the Galois field and finite field, e.g., see Hansen et al (Ref. B). Kelley et al's sum output is available. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to design the claimed invention according to Kelley et al's teachings because the circuit is a multiplication/accumulation capable of performing sum of product in single clock cycle as claimed.

Due to the similarity of independent claim 5 to the combination of claim 2 & 3, it is rejected under a similar rationale.

As per dependent claims 6-8, the claims add the detail features which are obvious to a person having ordinary skill in the art.

As per claims 9-13, the claims recite cipher circuits having multipliers as claimed in claims 1 & 5. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to design the claimed invention according to Kelley

Art Unit: 2193

et al's teachings because the multiplier circuit can be used in Galois field / finite field device as claimed.

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Cited references are art of interest.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tan V. Mai whose telephone number is (571) 272-3726. The examiner can normally be reached on Mon-Wed and Fri. from 9:30am to 2:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An, can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is:

Official (571) 273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.



Tan V. Mai  
Primary Examiner